International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 2 pp. 406-415 June 2019-Dec 2019 www.csjournals.com

Review on Security Challenges of Data Communication in IoT devices

Amanpal Singh Rayat[1], Inderjit Singh[2], Kamaljeet Singh[3]
[1,2,3]Assistant Professor, Faculty of computational Sciences, GNA University, Phagwara

Abstract: In current era, technology and information are playing the crucial role in day to day life. With the advancement of technology which is possible to connect various devices with the help of internet connectivity ranging from IP cameras to IoT devices. IoT infrastructure supports device to device (D2D) communication which is different from human to machine communication. IoT is a system which consists of machines, computational devices, objects and people are assigned with distinct identifiers and transfer the data over the internet without requiring human to machine interaction. The survey of statista.com in 2015 has been revealed that 75.44 billion devices are expected to be connected to the internet. Therefore, the security parameters should be needed in IoT network. In this paper, we discuss about the numerous attacks on the IoT protocol stack which was given by IETF and IEEE. We find out the possible attacks which are hazardous to the IoT devices, are based on categories the layer defined in the model. Also, we provide various countermeasures of these specified attacks, are a major concern.

Keywords: IoT, IoT attacks, IoT Security.

I. Introduction

The modern era is the internet, not only human beings need internet for communication but also all electronic devices should be required the internet connection, which is controlled by people from any remote location. With the emergence of technology that support high bandwidth and various transmission media techniques such as 4G, Wi-Fi, WiMax, and Broadband that IoT infrastructure came into existence. Since the technology and the IT service have been rampant, IoT devices has also surged in short span of time. IoT is myriad intelligent devices connected over network to serve human being.

In [1], authors define the IoT as “a world where physical objects are seamlessly integrated in to the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these ‘smart object’ over the Internet, query their state and any information associated with them, taking into account security and privacy issues”.

IoT network is considering complex as it consists of intelligent devices, actuator, sensors and Internet connectivity. The devices can be spread in any geographical area, appliances and portable devices.

The sensors in IoT networks capture the data and sent to the destination point for the processing of the data. The IETF and IEEE have given the specification of the IoT protocol stack to ensure the interoperability with the current devices using the internet. [2]

Application (CoAp, MQTT,XMPP,AMQP)
Transport (UDP,TCP)
Network and Routing (IPv4 and IPv6 /RPL)
Adaption (6LoWPAN)
Access Control (802.15.4, Bluetooth, ZigBee,NFC,LTE)
Physical (802.15.4, Radio)

Figure 1: IoT Protocol Stack

The IoT protocol stack in figure consists of various interoperable protocols:

(i) Physical Layer protocol consist of 802.15.4 (LR-WPANs; Low Rate Wireless Personal Area Networks): This is simple protocol supports low data rate with long battery time. It works on licence free frequency band which consists of sensors in remote controls, electronic toys, home automation etc.

(ii) Access Control Layer consists of NFC, Wi-Fi, LTE, Bluetooth, Zigbee etc. protocols used in media access control.

(iii) Network and Routing Layer consists of IPv4 and IPv6 over 6LoWPAN (Low-Power Wireless Personal Area Networks) [3] and RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) as the routing protocols.

(iv) Transport Layer consists of the UDP (User datagram protocol) or TCP (Transmission control protocol)

(v) Application Layer consists of several protocols like CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), MQTT (Message Queue Telemetry Transport), AMQP (Advanced Message Queuing Protocol) etc.

While the general scenario human to machine (H2M) communication is required, large network of devices machine to machine (M2M) communication should be needed.

IoT security is one of the hottest research areas these days. Numerous researchers around the globe are utilizing their endeavour to address different security issues and challenges in IoT. IoT security is an incredible issue which are challenging for many researchers as it deals with heterogeneous network and devices. IoT being the mix of such a significant number of devices have their own customary security.

II. Security Issues and Attacks in IoT System

In today's information era, the security is the central concern. In IoT infrastructure the sensors and actuators are mostly communicate on unguided media in order that the major security issues. The IoT devices are facing many challenges to cover the security lapses. For the secure communication over the network, the general CIA principal is based on a concept that is confidentiality, Integrity and Authentication. CIA alone is not sufficient for IoT environment [4], the more concrete IAS-octave which has to implement Information, Assurance and Security. The following table describe the security aims proposed by the IAS octave.

Table 1: IoT Security Requirements

Security Requirements	Definition
Confidentility	The process in which only authorized objects or users can get access to the data
Integrity	The process in which data completeness, and accuracy is preserved
Non repudiation	The process in which an IoT system can validate the incident or non-incident of an event
Availability	An ability of an IoT system to make sure its services are accessible, when demanded by authorized objects or users
Privacy	The process in which an IoT system follows privacy rules or policies and allowing users to control their sensitive data
Auditability	Ensuring the ability of an IoT system to perform firm monitoring on its actions
Accountability	The process in which an IoT system holds users taking charge of their actions.
Trustworthiness	Ensuring the ability of an IoT system to prove identity and confirm trust in third party

After defining the security requirements in IoT environment, the Security threats can be describe as the attack that violates the even one of the security requirement on IoT environment.

III. Taxonomy of IoT Attacks

1. **Physical Layer attacks**: This layer is easily to vulnerable because attacker, intruder and hacker are able to control the all physical IoT hardware such as controllers, sensors, RFID's ,which is the part of physical layer attacks. These attacks can be categories as follows:

- **Replication of device/ Tag cloning**: The attackers may be attacked by using a fake node or device in the IoT network; they do take place several attacks such as middle attack or denial of service attack and so on.

- **Physical Damage**: The devices like sensors, nodes, actuators may not be installed in those places where attacker can easily accessible. The attacker may harm the IoT hardware physically resulting in loss of information.

- **Sybil Attack:** While this attack is same as replication of device, each node claims numbers of fake identities in the context of network nodes.

- **Object tampering**: The attacker accesses the physical device in IoT network to launch the attack such as recovering the cryptographic keys, circuit modification, altering the firmware or operating system.

- **Social Engineering**: It is the process of acquiring the information such as password via social network. The attacker can acquire password or some technical information by simply communicating with the network administrator or technical person.

- **Side channel attack**: The attacker can exploit the channel information such as power consumption, network time and electromagnetic radiation to attack encryption mechanism.

2. **Access Control Layer attacks**: The attackers in this layer trying to take access, block or disturb the media on which IoT network works. IoT networks use Radio frequency, Bluetooth, ZigBee, NFC, LTE etc. The attacker tries to exploit the frequency to gain access to the network. Some of the types of attacks are as follows:

   - **Radio frequency interference on RFID's**: The main aim of this attack is to disturb the IoT network communication by sending many signals on same frequency range at which IoT network works.

   - **Outage attack**: By launching the different attacks which use huge energy from IoT network may power off some of the devices placed in unattached environment. This happens due to power outage.

   - **Signal Jamming**: Wireless communication works on specific frequency, its signal can be blocked by using jammers. Jammers block the frequency, therefore, making media unavailable for the communication.

   - **Camouflage / Spoofing**: The attacker can control the system using the RFID tag, and can inject the fake data on the IoT network.

- **Tracking**: It is the biggest threat to the privacy in terms of node. The movement of node is tracked and use to replicate the exactly the same profile of that particular node.

- **Unauthorized access**: The RFID authentication mechanism is not strong and vulnerable. This can be exploited by intruder to gain unauthorized access to the network.

- **Eavesdropping**: The small memory is used in IoT network. Thus, strong encryption and decryption mechanism cannot be implemented in this requirement with cost of speed. This leads to the eavesdropping, generally capturing the data between RFID tag and receiver.

- **Man in the middle (MITM)**: This attack is similar to the eavesdropping. This attack not only accesses the data but also can modify. In most cases, the receiver may get forged data.

- **Tag Killing**: Kill command is use to kill or stop the communicating node. This command should be protected by root/ super user strong password.

- **NFC based attacks**: This technology is used to exchange the data between the devices with same technology placed a shorter distance. NFC lacks of the protection techniques. It is vulnerable to eavesdropping, Relay attack (forwarding the request of victim's to a unauthorized person), Min in the middle attack,

- **Bluetooth based attacks**: In Bluetooth the security issues are very high due to the process of paring of devices to initiate the communication. During this initiation process several attacks based on the version of Bluetooth can be launched. Some of the vulnerabilities are as follows[7]:

    - If link keys are not properly managed or stored, then it would lead to revel to the attacker.

    - The length of encryption key length is allowed to be less than 1 byte, which is vulnerable.

    - Device authentication is done without user authentication.

  There are attacks like

    - Blue bugging which can take over the control on the node due to firmware vulnerability.

    - Blue jacking is exploiting the feature of sending the vCard and taking down the security.

    - Hijacking is done by attacking the configuration layer of iBeacon resulting in DoS and spoofing.

- **Wi-Fi based attacks**: Wi-Fi is vastly used in home automation / office automation using IoT. The possible attacks on the Wi-Fi network are as follows:

    - Dictionary attack: This attacker attempt to try different passwords from large set of passphrase also known as dictionary in this case.

    - WEP (Wired Equivalent Privacy) vulnerabilities, attacker recovers the encryption key by knowing the IV (initial vector) of stream cipher this is also known as FMS (Fluhere, Shamir and Mantin) attack. The replay protection is absent in CRC 32 checksum, the attacker encrypt the own message without knowing the encryption key known as Chopchop attack.

    - Google reply attack is perform by making google.com as home page and key stream was discover from the google.com log whenever user open google.com.

    - ARP spoofing: The attacker can send the fake ARP request with his own MAC address after the request all the ARP tables get updated. Now the user can send the packets to the attacker's MAC address instead of the access point of the network.

- **ZigBee based attack**: ZigBee is wireless net technology claim to consume less power. It is IEEE 802.15.4 standard defining only physical layer and MAC (Medium access control) ZigBig alliance provide the network (NWK) layer with API standardization [8]. The encryption keys are store in plain text; if intruder got physical access he can dump the memory to extract the keys. Moreover the network is vulnerable to the DoS (Denial of Service attack) with software like AmartRF Studio 7 [9].

3. **Network and Routing Layer attacks**: At this layer the hacker or intruder tries to exploit the vulnerabilities of network layer protocols to take control or disrupt the communication. The some of the attack are as follows:

    - RPL (Routing Protocol for Low Power and Lossy Network) based attacks mainly focus on disturbing the routing path and traffic. Some of the attacks are Selective forward attack, Wormhole attack, Blackhole attack, Hello flooding attack etc.

- 6loWPAN ((IPv6 over Low Power and Wireless Private Area Network) based attacks are DoS (Denial of service) and Wormhole Attack. This protocol is light-weighted and designed especially for IoT networks [11].

- Heterogeneity problem: Due to rise in the IoT devices, different types of protocols are implemented in IoT infrastructure. The default setting are at minimum and open for editing, resulting in the invitation to attacks/ exploits.

4. **Transport Layer attacks**: The major attacks on this layer is on the TCP and UDP protocols as these are the major protocols used in this layer of IoT stack. The common attacks on this layer as under:

   - **TCP-UDP Port scanning**: The attacker sends message to each port to check that if the ports are open.

   - **UDP flooding**: The attacker sends large number of UDP packet to various random ports making the some object unreachable. It is similar to the DoS attack.

   - **TCP Hijacking**: The attacker observer the TCP session and trying to get/ hijack the sequence number and checksum. If he is successful then he introduce malicious TCP packet into the network with the hijacked information.

   - **TCP SYN flooding**: The attacker frequently sending the SYN packets, to initiate the connection resulting in slow down the node. This attack also DoS type of attack.

   - **TCP-UDP fragmentation:** This a DoS attack; the packets of large size greater than the MTU (maximum transmission unit) is send consuming the resources of the network and it will be very hard to distinguish from other packet data units.

5. **Application layer protocols-based attacks**: The protocols used at this layer are CoAP, MQTT, XMPP, AMQP among these MQTT and CoAP are widely used at this layer. The intruders launches the following attacks:

   - **Pre-shared key attack:** The Constrained Application Protocol (CoAP) use pre-shared keys for the communication. The attacker can get those keys if he got access to the library files.

   - **Beast:** This attack exploits the vulnerability in TLS (Transport Layer Security) 1.0. The attacker may make use of CBC (Cipher Block Chaining) to decrypt the cookies or part of message.

- **Diffie-Hellman Parameters:** Almost all the TLS versions have the vulnerable to cross-protocol attack; while exchanging keys with Diffie-Helman method.
- **Klima03:** SSL (Secure Socket Layer) / TLS could be decrypted if the attacker got the pre-master secrete value in RSA or certificate.
- **Xmpp bomb:** This is a DoS attack in which attacker sends the request consist of white spaces.
- **Man in the middle (MITM) attack:** It can be launched on MQTT as it sends the username and password in un-encrypted form.
- **Buffer Overflow:** It can exploit the vulnerability of open port on MQTT protocol.
- **Account hijacking:** The attacker can use social engineering or other technique to reveal the user login resulting in compromising the security of network.

Apart from these attacks, we have Malware attack, Operating System based attack, Firmware-based attacks etc.

IV. Security measures:

Physical and Access Control level: The IoT network works on radio frequency (wireless) making the more vulnerable to attacks discussed in Physical layer attacks, as compare to the wired media. To make the network hard to crack the following technique can be implemented:

- Frequency Hopping Spread Spectrum (FHSS): It is the method in which the data is send over radio signal with varying frequency channels, the variation sequence is already agreed upon by the sender and receiver. This will had to tune with the frequency for the intruder and making hard to penetrate into the network. The only limitation is that, we need much wider frequency bandwidth.
- Use of timestamps, onetime passwords, cryptography, Trusted Certification etc. for Sybil attacks.
- Location/Position Verification, Received Signal Strength Indicator (RSSI): based scheme would be implemented for the tag cloning and side Channing attack.
- Random Key Redistribution for the authenticating and creating the session for the communication.

Network and Routing: IoT is having more challenges as compare to the internet; In internet the human is accessing the machines (servers and resources) whereas the IoT is link between machine to machine access. It is more challenging to authenticate the devices leaving the possibility of Man in the Middle Attack. The node protecting is key concern in IoT network and can be done by developing the more robust protocols and authentication mechanism.

Transport level: In this layer most of the attackers do port scanning to attack. For the security you can block the ports using firewall but still it is not possible to block the port scanning. The use of honeypots technique would be very useful in this case. In this deceptive defence technique the firewall will be redirecting the port to the empty hosts / honeypots.

Application level: In this layer the IDS (Intrusion Detection System) could be implemented to deal with the threats discussed so far. IDS systems are signature based/ misuse and anomaly detection. Many hybrid variant has been proposed but none is prove to be concrete solution against DoS attacks. Few attacks like SQL injection, XXS, Misconfiguration can be taken care of by using standard and updated guidelines and patches for application development.

V. Conclusion

As IoT system mostly works on the wireless network, it can be considered that it is vulnerable to the attacks as compared to the wired network. The intense work is needed in future for securing the network from the Physical and Access Control Layer attacks; these are the lower layer of IoT protocol stacks and should be fortified against the intruders. As the advancement of computing power, it is easy to override the weak network i.e. IoT. The various attacks such as Tag cloning, Sybil attack and side channel attack at physical layer could be fortified by using FHSS and RSSI techniques. The attacks at access control layer should be secured by developing light weight authentication protocols.

VI. References

1. S. Haller, S. Karnouskos, and C. Schroth,“The Internet of Things in an Enterprise Context,” in Future Internet – FIS 2008, vol. 5468ofLectureNotesinComputer Science,pp.14–28,Springer BerlinHeidelberg,Berlin,Heidelberg,2009.
2. J. Granjal, E. Monteiro, and J.S´aSilva, “Security for the internet of things: a survey of existing protocols and open research issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp.1294–1312, 2015.
3. A.Zanella, N.Bui, A.P.Castellani, L.Vangelista, and M.Zorzi, “Internet of things for smart cities,” IEEE Internet of Things Journal, vol.1, no.1, pp.22–32, 2014.
4. Hezam Akram Abdul-Ghani, Dimitri Konstantas , Mohammed Mahyoub “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model” International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018
5. Inayat Ali, Sonia Sabir1, Zahid Ullah, “Internet of Things Security, Device Authentication and Access Control: A Review”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016
6. C. Ramakrishna, G. Kiran Kumar, A. Mallikarjuna Reddy, Pallam Ravi “A Survey on various IoT Attacks and its Countermeasures”, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018
7. Peter Cope, Joseph Campbell, Thaier Hayajneh, “An Investigation of Bluetooth Security Vulnerabilities”, 978-1-5090-4228-9/17/$31.00 ©2017 IEEE
8. Wei Wang, Guangyu He, Junli Wan, “Research on Zigbee wireless communication technology”, The National Natural Science Foundation of China
9. Ing. Ján Ďurech, prof. Ing. Mária Franeková, “Security attacks to ZigBee technology and their practical realization”, IEEE 12th International Symposium on Applied Machine Intelligence and Informatics.

10. Snehal Deshmukh-Bhosale, Santosh S. Sonavane, "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things", The 12th International Conference Interdisciplinary in Engineering.
11. https://tools.ietf.org/html/rfc7252
12. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)
13. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ as on 31 Oct 2019